EXHIBIT J

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	The Ruckus Devices comprise wireless access points and routers that provide Quality of Service ("QoS") support in accordance with Wi-Fi Multimedia (WMM) and IEEE 802.1p and 802.11e standards. The Ruckus Devices include, but are not limited to the R730. The Ruckus Devices perform a method for checking permissibility to use a service. The Ruckus Devices use QoS to check the permissibility of the transmission of a packet stream (e.g., Voice, Video, etc.) in a communications network. 

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**NEW RUCKUS R730 IS THE FIRST IOT- AND LTE-READY 802.11AX ACCESS POINT FOR STADIUMS, PUBLIC VENUES, TRAIN STATIONS AND SCHOOLS** Company also launches Ultra-High Density Technology Suite that enhances network performance and WPA3 security compliance to protect end-users from common attacks **SUNNYVALE, Ca., July 17, 2018** – Ruckus Networks, an ARRIS company, today announced the Ruckus R730, the industry's first IoT- and LTE-ready, 802.11ax wireless access point (AP). The high-capacity, 12 spatial-stream R730 works in concert with the new Ruckus Ultra-High Density Technology Suite to smoothly deliver high-resolution, latency-sensitive video in ultra-high density user environments such as stadiums, train stations and schools. In addition, the R730 complies with both the new WPA3™ security protocol and Wi-Fi™ Enhanced Open for more secure connections on public networks. Worldwide data and video traffic is growing at double-digit rates, driven by an increase in connected devices. ABI Research predicts that Wi-Fi device shipments will grow to nearly 35 billion by 2022. Data and video traffic also will surge due to increased per-device data consumption driven by applications like 4K video streaming, virtual and augmented reality and live-stream gaming. "Ruckus customers and partners demand more when it comes to their networks," said Ian Whiting, president of Ruckus Networks. "We have a long history of delivering products and technologies that go beyond the current state-of-the-art to meet the world's most demanding network requirements while driving down the cost-per-connection. Ruckus R730 and Ruckus Ultra-High Density Technology Suite are the latest examples." The congestion of people, devices and bandwidth-hungry apps makes for challenges that current wireless tech cannot handle. Adding to the complexity of this environment are diversifying device categories and apps, such as instant messaging, IoT control messages and voice-over-Wi-Fi. "Real-world use cases are bumping up against the limits of existing Wi-Fi standards, and the need for 802.11ax to address a wide variety of heterogeneous, high-density scenarios is clear," said Chris DePuy, founder and technology analyst at 650 Group. "Ruckus has already differentiated itself in the realm of network consolidation. With this launch, Ruckus is reinforcing that by setting the stage for converged Wi-Fi, IoT and LTE deployments." **802.11ax: More connections and bandwidth, higher QoS** The new 802.11ax standard was designed for high-density connectivity, with the ability to support up to a four-fold capacity increase over its 802.11ac Wave 2 predecessor. With 802.11ax, multiple APs used in dense device environments are collectively able to deliver required quality-of-service (QoS) to more clients with more diverse usage profiles due to the use of orthogonal frequency-division multiple access (OFDMA) and multi-user multiple-in multiple-out (MU-MIMO) technologies. **Source: https://www.ruckuswireless.com/press/releases/20180717-new-ruckus-r730-first-iot-and-lte-ready-80211ax-access-point-stadiums-public**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	# Quality of Service ## Quality of Service overview Quality of Service (QoS) provides preferential treatment to specific traffic. Quality of Service (QoS) features are used to prioritize the use of bandwidth in a switch. When QoS features are enabled, traffic is classified as it arrives at the switch, and processed through on the basis of configured priorities. Traffic can be dropped, prioritized for guaranteed delivery, or subject to the delivery options as configured by a number of different mechanisms. *Classification* is the process of selecting packets on which to perform QoS, reading or ignoring the QoS information, and assigning a priority to the packets. The classification process assigns a priority to packets as they enter the switch. These priorities can be determined on the basis of information contained within the packet or assigned to the packet as it arrives at the switch. Once a packet or traffic flow is identified and marked, then it is mapped to a forwarding priority queue. Packets on Ruckus devices are classified in up to eight traffic classes with values from 0 to 7. Packets with higher priority classifications are given a precedence for forwarding. There are two traffic types in QoS: • Data—These can be either network-to-network traffic or traffic from the CPU. QoS parameters can be assigned and modified for data traffic. The device also supports setting or modifying the IEEE 802.1p user priority or the IP header DSCP field.. • Control—Packets to and from the CPU is considered control traffic. The QoS parameters associated with the control traffic are preassigned and not configurable. **Source: Ruckus FastIron QoS and Traffic Management Configuration Guide, 08.0.90, p. 11**

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:</td><td>
TABLE 13 Default bandwidth for combined SP and WRR queueing methods
<table>
<tr><th>Queue</th><th>Default bandwidth</th></tr>
<tr><td>qosp7</td><td>Strict Priority (highest priority)</td></tr>
<tr><td>qosp6</td><td>Strict Priority</td></tr>
<tr><td>qosp5</td><td>25%</td></tr>
<tr><td>qosp4</td><td>15%</td></tr>
<tr><td>qosp3</td><td>15%</td></tr>
<tr><td>qosp2</td><td>15%</td></tr>
<tr><td>qosp1</td><td>15%</td></tr>
<tr><td>qosp0</td><td>15% (lowest priority)</td></tr>
</table>
Source: Ruckus FastIron QoS and Traffic Management Configuration Guide, 08.0.90, p. 24
</td></tr>
</table>

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**The Ruckus Devices implement the service (e.g. VoIP, Video, etc.) in at least one communications network (e.g., 802.11 network).** **Quality of Service overview** Quality of Service (QoS) provides preferential treatment to specific traffic. Quality of Service (QoS) features are used to prioritize the use of bandwidth in a switch. When QoS features are enabled, traffic is classified as it arrives at the switch, and processed through on the basis of configured priorities. Traffic can be dropped, prioritized for guaranteed delivery, or subject to the delivery options as configured by a number of different mechanisms. *Classification* is the process of selecting packets on which to perform QoS, reading or ignoring the QoS information, and assigning a priority to the packets. The classification process assigns a priority to packets as they enter the switch. These priorities can be determined on the basis of information contained within the packet or assigned to the packet as it arrives at the switch. Once a packet or traffic flow is identified and marked, then it is mapped to a forwarding priority queue. Packets on Ruckus devices are classified in up to eight traffic classes with values from 0 to 7. Packets with higher priority classifications are given a precedence for forwarding. There are two traffic types in QoS: • Data—These can be either network-to-network traffic or traffic from the CPU. QoS parameters can be assigned and modified for data traffic. The device also supports setting or modifying the IEEE 802.1p user priority or the IP header DSCP field.. • Control—Packets to and from the CPU is considered control traffic. The QoS parameters associated with the control traffic are preassigned and not configurable. **Source: Ruckus FastIron QoS and Traffic Management Configuration Guide, 08.0.90, p. 11**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, **the communication network having an overall transmission capacity**, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	The communications network provided by the Ruckus Devices has an overall transmission capacity. The overall transmission capacity is the capacity of the 802.11 network. (see Wi-Fi table below) Source: Ruckus R730 Data Sheet, p. 3

WI-FI	
Wi-Fi Standards	• IEEE 802.11a/b/g/n/ac/ax
Supported Rates	• 802.11ax: 4 to 4800 Mbps • 802.11ac: 6.5 to 3467 Mbps • 802.11n: 6.5 to 600 Mbps • 802.11a/g: 6 to 54 Mbps • 802.11b: 1 to 11 Mbps
Supported Channels	• 2.4GHz: 1-13 • 5GHz: 36-64, 100-144, 149-165
MIMO	• 8x8 MU-MIMO • 8x8 SU-MIMO
Spatial Streams	• 8 MU-MIMO • 8 SU-MIMO
Radio Chains and Streams	• 8x8:8
Channelization	• 20, 40, 80MHz
Modulation	• OFDMA (up to 1024-QAM)
Security	• WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i, Dynamic PSK • WIPS/WIDS
Other Wi-Fi Features	• WMM, Power Save, TxBF, LDPC, STBC, 802.11r/k/vHotspot • Hotspot 2.0 • Captive Portal • WISPr

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:</td><td>The use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network. The Ruckus Devices transmit at least one service-specific traffic stream, for example the traffic stream related to voice/video/background etc. The traffic stream is assigned to the service by the Ruckus Device. The Ruckus Device is assigned to service the 802.11 network.

TC traffic category is a label for MSDUs that have a distinct user priority as viewed by higher layer entities for delivery over the same link. MAC entities determine the priority value for MSDUs that belong to a particular traffic category by using the priority value provided with the MSDU at the MAC service access point.

TABLE 13 Default bandwidth for combined SP and WRR queueing methods
<table><tr><th>Queue</th><th>Default bandwidth</th></tr><tr><td>qosp7</td><td>Strict Priority (highest priority)</td></tr><tr><td>qosp6</td><td>Strict Priority</td></tr><tr><td>qosp5</td><td>25%</td></tr><tr><td>qosp4</td><td>15%</td></tr><tr><td>qosp3</td><td>15%</td></tr><tr><td>qosp2</td><td>15%</td></tr><tr><td>qosp1</td><td>15%</td></tr><tr><td>qosp0</td><td>15% (lowest priority)</td></tr></table>
Source: Ruckus FastIron QoS and Traffic Management Configuration Guide, 08.0.90, p. 24</td></tr>
</table>

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:</td>
<td>Table 9-1—UP-to-AC mappings
<table>
<tr><th>Priority</th><th>UP (Same as 802.1D user priority)</th><th>802.1D designation</th><th>AC</th><th>Designation (informative)</th></tr>
<tr><td>Lowest</td><td>1</td><td>BK</td><td>AC_BK</td><td>Background</td></tr>
<tr><td></td><td>2</td><td>—</td><td>AC_BK</td><td>Background</td></tr>
<tr><td></td><td>0</td><td>BE</td><td>AC_BE</td><td>Best Effort</td></tr>
<tr><td></td><td>3</td><td>EE</td><td>AC_BE</td><td>Best Effort</td></tr>
<tr><td></td><td>4</td><td>CL</td><td>AC_VI</td><td>Video</td></tr>
<tr><td></td><td>5</td><td>VI</td><td>AC_VI</td><td>Video</td></tr>
<tr><td></td><td>6</td><td>VO</td><td>AC_VO</td><td>Voice</td></tr>
<tr><td>Highest</td><td>7</td><td>NC</td><td>AC_VO</td><td>Voice</td></tr>
</table>
Source: https://standards.ieee.org/standard/802_11-2012.html</td></tr>
</table>

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:</td><td>

I.4 Traffic types and priority values

Table I-2 shows the correspondence between traffic types and priority values used to select the defaults in Table 8-5. The default priority used for transmission by end stations is 0. Changing this default would result in confusion and likely in interoperability problems. At the same time, the default traffic type is definitely Best Effort. 0 is thus used both for default priority and for Best Effort, and Background is associated with a priority value of 1. This means that the value 1 effectively communicates a lower priority than 0.

Table I-2—Traffic type acronyms

Priority	Acronym	Traffic type
1	BK	Background
0 (Default)	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	"Video," < 100 ms latency and jitter
5	VO	"Voice," < 10 ms latency and jitter
6	IC	Internetwork Control
7	NC	Network Control

Source: https://standards.ieee.org/standard/802_1Q-2018.html
</td></tr>
</table>

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**I.1 Traffic types** A full description of the QoS needs of applications and network services is too complex to be represented by a simple number 0 through 7. The pragmatic aim of traffic classification is to simplify requirements to preserve the high-speed, low-cost characteristics of Bridges. At the margin, potential bandwidth efficiency is traded for simplicity and higher speed operation—historically a good decision in the LAN. The following list of traffic types, each of which can benefit from simple segregation from the others, are of general interest: a) Network Control—characterized by a guaranteed delivery requirement to support configuration an maintenance of the network infrastructure. b) Internetwork Control—in large networks comprising separate administrative domains there is typically a requirement to distinguish traffic supporting the network as a concatenation of those domains from the Network Control of the immediate domain. c) Voice—characterized by less than 10 ms delay and, hence, maximum jitter (one way transmission through the LAN infrastructure of a single campus). d) Video—characterized by less than 100 ms delay, or other applications with low latency as the primary QoS requirement. e) Critical Applications—characterized by having a guaranteed minimum bandwidth as their primary QoS requirement and subject to some form of admission control to ensure that one system or application does not consume bandwidth at the expense of others. The admission control mechanism can range from preplanning of the network requirement at one extreme to bandwidth reservation per flow at the time the flow is started at the other. f) Excellent Effort—or "CEO's best effort," the best-effort type services that an information services organization would deliver to its most important customers. g) Best Effort—for default use by unprioritized applications with fairness only regulated by the effects of TCP's dynamic windowing and retransmission strategy. h) Background—bulk transfers and other activities that are permitted on the network but that should not impact the use of the network by other users and applications. **Source: https://standards.ieee.org/standard/802_1Q-2018.html** 6.5.9 Priority The MAC Service includes priority as a QoS parameter. MA_UNITDATA.request primitives with a high priority may be given precedence over other request primitives made at the same station, or at other stations attached to the same LAN and can give rise to earlier MA_UNITDATA.indication primitives. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**35. Stream Reservation Protocol (SRP)** SRP utilizes three signaling protocols, MMRP (10.9), MVRP (Clause 11) and MSRP (35.1), to establish stream reservations across a bridged network. Within SRP the Multiple MAC Registration Protocol (MMRP) is optionally used to control the propagation of Talker registrations throughout the bridged network (35.2.4.3.1). The Multiple VLAN Registration Protocol (MVRP) is used by end stations and Bridges to declare membership in a VLAN where a Stream is being sourced. This allows the Data Frame Priority (35.2.2.8.5(a)) to be propagated along the path from Talker to Listener(s) in tagged frames. MSRP will not allow Streams to be established across Bridge Ports that are members of the untagged set (8.8.10) for the related VID. The Multiple Stream Registration Protocol (MSRP) is a signaling protocol that provides end stations with the ability to reserve network resources that will guarantee the transmission and reception of data streams across a network with the requested QoS. These end stations are referred to as Talkers (devices that produce data streams) and Listeners (devices that consume data streams). **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
A method for checking permissibility to use a service, the service being implemented in at least one communications network, the communication network having an overall transmission capacity, the use of the service comprising transmission of at least one service-specific traffic stream which is assigned to the service by an access node which is assigned to the service to the communication network, comprising:	**35.1 Multiple Stream Registration Protocol (MSRP)** MSRP supports the reservation of resources for streams, each destined for one or more Listeners, and each from a single source, across a bridged network. Transmitted data that conforms to a successful stream reservation will not be discarded by any Bridge due to congestion on a LAN. In order to propagate requests for reservations, MSRP defines an *MRP application* that provides the Stream resource registration service defined in 35.2.3. MSRP makes use of the MRP Attribute Declaration (MAD) function, which provides the common state machine descriptions defined for use in MRP-based applications. The MRP architecture, and MAD are defined in Clause 10. MSRP defines a new MRP Attribute Propagation (MAP) function, to provide an attribute propagation mechanism. MSRP propagates registrations for stream reservations in a manner similar to the operation of MMRP (10.9) and MVRP (11.2), which are used for registering Group membership and individual MAC address information, and VLAN membership, respectively. Unlike MMRP and MVRP, however, the registered attributes can be combined, discarded, or otherwise altered, as they are propagated by the participating Bridges. In order to make and keep QoS guarantees all devices in a bridged network must participate in the signaling and queuing operations required of Bridges. For example, this would include IEEE 802.11 wireless media access points and stations. Thus, MSRP provides a means for Bridges or end stations running MSRP to cooperate both with higher network layers, such as routers or hosts running RSVP, and with lower network layers, such as wireless media. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	The Ruckus Devices analyze the use of the service with an access control function which is assigned to the access node. The Ruckus Devices analyze the service (e.g., voice/video/background) with an access control function (e.g., the function resulting from a call to the ADDTS function) which is assigned to the access node. The ADDTS function results in analysis of the use of the service via the TSPEC element defined in the primitive, TSPEC element further contains information about the QOS parameters. **6.3.26.2.3 When generated** This primitive is generated by the SME to request the addition of a new (or modification of an existing) TS in order to support parameterized QoS transport of the MSDUs belonging to this TS when a higher layer protocol or mechanism signals the STA to initiate such an addition (or modification). **6.3.26.2.4 Effect of receipt** The STA operates according to the procedures defined in 10.4. **6.3.26.3 MLME-ADDTS.confirm** **6.3.26.3.1 Function** This primitive reports the results of a TS addition (or modification) attempt. **6.3.26.3.2 Semantics of the service primitive** The primitive parameters are as follows: MLME-ADDTS.confirm(ResultCode, DialogToken, TSDelay, TSPEC, Schedule, TCLAS, TCLASProcessing, EBR, VendorSpecificInfo) Source: https://standards.ieee.org/standard/802_11-2012.html

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>analyzing the use of the service with an access control function which is assigned to the access node; and</td><td>
6.3.26.4 MLME-ADDTS.indication

6.3.26.4.1 Function

This primitive reports to the HC's SME the request for adding (or modifying) a TS.

6.3.26.4.2 Semantics of the service primitive

The primitive parameters are as follows:
MLME-ADDTS.indication (
DialogToken,
STAAddress,
TSPEC,
TCLAS,
TCLASProcessing,
U-APSD Coexistence,
EBR,
VendorSpecificInfo
)

<table>
<tr><th>Name</th><th>Type</th><th>Valid range</th><th>Description</th></tr>
<tr><td>DialogToken</td><td>Integer</td><td>As defined in the received ADDTS request frame</td><td>Specifies a number unique to the QoS Action primitives and frames used in adding (or modifying) the TS.</td></tr>
<tr><td>STAAddress</td><td>MACAddress</td><td></td><td>Contains the MAC address of the STA that initiated the MLME-ADDTS.request primitive.</td></tr>
</table>
Source: https://standards.ieee.org/standard/802_11-2012.html

8.5.3.2 ADDTS Request frame format

The ADDTS frames are used to carry TSPEC and optionally TCLAS elements to set up and maintain TSs using the procedures defined in 10.4.

The Action field of the ADDTS Request frame contains the information shown in Table 8-193.

Source: https://standards.ieee.org/standard/802_11-2012.html
</td></tr>
</table>

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>analyzing the use of the service with an access control function which is assigned to the access node; and</td><td>

Table 8-193—ADDTS Request frame Action field format

<table>
<tr><th>Order</th><th>Information</th></tr>
<tr><td>1</td><td>Category</td></tr>
<tr><td>2</td><td>QoS Action</td></tr>
<tr><td>3</td><td>Dialog Token</td></tr>
<tr><td>4</td><td>TSPEC</td></tr>
<tr><td>5–n</td><td>TCLAS (optional)</td></tr>
<tr><td>n + 1</td><td>TCLAS Processing (optional)</td></tr>
<tr><td>n + 2</td><td>U-APSD Coexistence (optional)</td></tr>
<tr><td>n + 3</td><td>Expedited Bandwidth Request element (optional)</td></tr>
</table>

The Category field is set to 1 (representing QoS).

The QoS Action field is set to 0 (representing ADDTS request).

The Dialog Token, TCLAS, and TCLAS Processing fields of this frame are contained in an MLME-ADDTS.request primitive that causes the frame to be sent. Some of the TSPEC parameters are contained in the MLME-ADDTS.request primitive while the other parameters (i.e., Surplus Bandwidth Allowance, Minimum Service Interval, Maximum Service Interval, and Minimum PHY Rate) are generated within the MAC.

The TSPEC element, defined in 8.4.2.32, and the optional TCLAS element, defined in 8.4.2.33, contain the QoS parameters that define the TS. The TS is identified by the TSID and Direction fields within the TSPEC element. The TCLAS element is optional at the discretion of the STA that sends the ADDTS Request frame, regardless of the setting of the access policy (EDCA or HCCA). There may be one or more TCLAS elements in the ADDTS frame. The TCLAS Processing element is present when there are more than one TCLAS element and is defined in 8.4.2.35. There may be one Expedited Bandwidth Request element, which is defined in 8.4.2.96.

The U-APSD Coexistence element, defined in 8.4.2.93, contains the coexistence parameters requested by the non-AP STA when using the U-APSD Coexistence capability as described in 10.2.1.5.2. The U-APSD Coexistence element is optionally present.

Source: https://standards.ieee.org/standard/802_11-2012.html

</td></tr>
</table>

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	**5.2.2.2 Semantics of the service primitive** The parameters of the primitive are as follows: MA-UNITDATA.request(source address, destination address, routing information, data, priority, service class) The source address (SA) parameter specifies an individual MAC sublayer address of the sublayer entity from which the MSDU is being transferred. The destination address (DA) parameter specifies either an individual or a group MAC sublayer entity address. The routing information parameter specifies the route desired for the data transfer (a null value indicates source routing is not to be used). For IEEE Std 802.11, the routing information parameter shall be null. The data parameter specifies the MSDU to be transmitted by the MAC sublayer entity. For IEEE Std 802.11, the length of the MSDU shall be less than or equal to 2304 octets. The priority parameter specifies the priority desired for the data unit transfer. The allowed values of priority are described in 5.1.1.4. The service class parameter specifies the service class desired for the data unit transfer. The allowed values of service class are described in 5.1.1.5 and 5.1.3. **Source: https://standards.ieee.org/standard/802_11-2012.html**

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	**5.2.2.4 Effect of receipt** On receipt of this primitive, the MAC sublayer entity determines whether it is able to fulfill the request according to the requested parameters. A request that cannot be fulfilled according to the requested parameters is discarded, and this action is indicated to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive that describes why the MAC was unable to fulfill the request. If the request can be fulfilled according to the requested parameters, the MAC sublayer entity appends all MAC specified fields (including DA, SA, FCS, and all fields that are unique to IEEE Std 802.11), passes the properly formatted frame to the lower layers for transfer to a peer MAC sublayer entity or entities (see 5.1.4), and indicates this action to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive with transmission status set to Successful. **Source: https://standards.ieee.org/standard/802_11-2012.html** **34.2 Detection of SRP domains** The concept of audio/video (AV) streams, the Stream Reservation Protocol (SRP), and the traffic forwarding and shaping functions that support stream transmission (see 6.9.4 and 8.6.8.1), rely on the ability of each Bridge to detect whether each of its ports is at the edge of a region of connected Bridges that support SRP on a particular priority, so that the Priority Code Point values associated with traffic entering an *SRP domain* (3.257) can be properly regenerated at the boundary of the domain, as described in 6.9.4. Bridges detect the edge of an SRP domain by observing SRP behavior. If a Bridge receives SRP registrations using a particular priority, then it is reasonable to believe that they are being received from an SRP-capable device; the SRP engine can therefore signal which Ports of a Bridge are at the boundary of an SRP domain. The per-port, per-SR class, *SRPdomainBoundaryPort* parameter determines whether a Port is considered to be at the edge of an SRP domain or within the core of the domain, as defined in 35.1.4. This parameter is controlled by the operation of SRP. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	**34. Forwarding and Queuing Enhancements for time-sensitive streams (FQTSS)** 34.1 Overview This clause describes a set of tools that can be used to support the forwarding and queuing requirements of time-sensitive streams. In this context, a "time-sensitive stream" is taken to be a stream of traffic, transmitted from a single source station, destined for one or more destination stations, where the traffic is sensitive to timely delivery, and in particular, requires transmission latency to be bounded. Such streams include video or audio data streams, where there is a desire to limit the amount of buffering required in the receiving station. NOTE 1—An example of this requirement would be a live performance where a video image of the performance is simultaneously projected on a screen in the auditorium, and it is desirable for the sound and image to be "in sync" with the performance. In order to address the needs of such traffic in Bridges, the following are provided: a) A means of detecting the boundary between a set of Bridges that support SRP (an SRP domain) and surrounding Bridges that do not support SRP. This mechanism is described in 34.2. NOTE 2—The primary intent of these functions is to support SRP; however, there is no specific interdependency between these functions and SRP, so they could equally be used to support other admission control mechanisms if they were implemented. b) A set of bandwidth availability parameters for each port that are used to record the maximum bandwidth available to a given outbound queue, and the actual bandwidth reserved, for that queue. These parameters are described in 34.3. c) A credit-based shaper algorithm, defined in 8.6.8.1, that is used to shape the transmission of stream-based traffic in accordance with the bandwidth that has been reserved on a given outbound queue. d) A discussion of the relationship between the size of the layer 2 "payload" (the MSDU) carried in a frame and how that relates to the actual bandwidth that will be consumed when that MSDU is transmitted on a particular Port (34.4). e) An algorithm for determining the mapping of the priorities associated with received frames onto the traffic classes available on the transmission Ports of a Bridge (34.5). f) A definition of the required behavior of an end station that acts as the source of a time-sensitive data stream (34.6). **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
analyzing the use of the service with an access control function which is assigned to the access node; and	**34.5 Mapping priorities to traffic classes for time-sensitive streams** In Bridges that support FQTSS, the default mappings of priorities to traffic classes meet the following constraints: a) Priority values that correspond to SR classes are mapped onto traffic classes that support the credit-based shaper algorithm as the transmission selection algorithm. b) Traffic classes that support the credit-based shaper algorithm have a higher priority than traffic classes that support the strict priority (or any other) transmission selection algorithm. c) At least one traffic class supports the credit-based shaper algorithm, and at least one traffic class supports the strict priority transmission selection algorithm. NOTE 1—The constraint that there is at least one traffic class that supports the strict priority transmission selection ensures that there is at least one traffic class that can support traffic that is not subject to bandwidth reservation, such as "best effort" traffic. The recommended default priority to traffic class mappings for a system that supports SR class A (using priority 3) and SR class B (using priority 2) are shown in Table 34-1. The recommended default priority to traffic class mappings for a system that supports only SR class B (using priority 2) are shown in Table 34-2. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

<table>
<tr><th>Claim 1</th><th>RUCKUS DEVICES</th></tr>
<tr><td>checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is</td><td>
The Ruckus Devices practice checking, via the access control function (e.g., MAC sublayer with ADDTS function), without further interrogations at internal transmission nodes of the communications network, whether the use of the service (e.g., voice/video/background) is permitted, the checking performed taking into account an available capacity, which is determined taking into account the overall transmission capacity (e.g., bandwidth parameters), and available to the access node for transmitting traffic streams to the communications network. As part of the Stream Reservation Protocl, the Ruckus Devices check to see if it can reserve the bandwidth and then passes the reservation request on to the next hop in the network.
The available admission capacity list comprises a sequence of available admission capacity fields, for the corresponding user priority or traffic. The ADDTS function does not interrogate the internal transmission nodes in the communication network when performing this check.
8.4.2.30 BSS Load element
The BSS Load element contains information on the current STA population and traffic levels in the BSS. The element information format is defined in Figure 8-191. This element may be used by the STA for vendor-specific AP selection algorithm when roaming.
<table>
<tr><td></td><td>Element ID</td><td>Length (5)</td><td>Station Count</td><td>Channel Utilization</td><td>Available Admission Capacity</td></tr>
<tr><td>Octets:</td><td>1</td><td>1</td><td>2</td><td>1</td><td>2</td></tr>
</table>
Figure 8-191—BSS Load element format
The STA Count field is interpreted as an unsigned integer that indicates the total number of STAs currently associated with this BSS.
Source: https://standards.ieee.org/standard/802_11-2012.html
</td></tr>
</table>

Claim 1	RUCKUS DEVICES
checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is	**34.3 The bandwidth availability parameters** The following bandwidth availability parameters exist for each Port, and for each traffic class, N, that supports the credit-based shaper algorithm: a) *portTransmitRate* as defined in 8.6.8.2; b) *deltaBandwidth(N)*: The additional bandwidth, represented as a percentage of *portTransmitRate*, that can be reserved for use by the queue associated with traffic class N, in addition to the *deltaBandwidth(N)* values associated with higher priority queues. For a given traffic class N, the total bandwidth that can be reserved is the sum of the *deltaBandwidth* values for traffic class N and all higher traffic classes, minus any bandwidth reserved by higher traffic classes that support the credit-based shaper algorithm (see 34.3.1). c) *adminIdleSlope(N)*: The bandwidth, in bits per second, that has been requested by management to be reserved for use by the queue associated with traffic class N. If SRP is in operation, this parameter has no effect; if SRP is not in operation, then the value of *operIdleSlope(N)* is always equal to the value of *adminIdleSlope(N)*. d) *operIdleSlope(N)*: The actual bandwidth, in bits per second, that is currently reserved for use by the queue associated with traffic class N. This value is used by the credit-based shaper algorithm (8.6.8.2) as the *idleSlope* for the corresponding queue. In all cases, bandwidth is defined in terms of the actual bandwidth consumed when frames are transmitted through the Port, not the size of the MSDU "payload" carried within those frames. Subclause 34.4 discusses the relationship between MSDU size and actual bandwidth consumed. NOTE—While the deltaBandwidth values are specified with respect to specific traffic classes, and indicate the amount of bandwidth that can be reserved for traffic belonging to a particular traffic class, this does not imply that these traffic classes have preferential access to that portion of the bandwidth. The priority of a given traffic class does not, for example, imply anything about the importance of a data stream that uses that class; the reservation strategy might therefore allocate bandwidth to a high importance stream that uses a lower priority traffic class in preference to a stream of lower importance that uses a higher priority traffic class. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is	**35. Stream Reservation Protocol (SRP)** SRP utilizes three signaling protocols, MMRP (10.9), MVRP (Clause 11) and MSRP (35.1), to establish stream reservations across a bridged network. Within SRP the Multiple MAC Registration Protocol (MMRP) is optionally used to control the propagation of Talker registrations throughout the bridged network (35.2.4.3.1). The Multiple VLAN Registration Protocol (MVRP) is used by end stations and Bridges to declare membership in a VLAN where a Stream is being sourced. This allows the Data Frame Priority (35.2.2.8.5(a)) to be propagated along the path from Talker to Listener(s) in tagged frames. MSRP will not allow Streams to be established across Bridge Ports that are members of the untagged set (8.8.10) for the related VID. The Multiple Stream Registration Protocol (MSRP) is a signaling protocol that provides end stations with the ability to reserve network resources that will guarantee the transmission and reception of data streams across a network with the requested QoS. These end stations are referred to as Talkers (devices that produce data streams) and Listeners (devices that consume data streams). **35.2.2.8.4 TSpec** The 32-bit TSpec component is the TSpec associated with a Stream. It consists of the following two elements (which are encoded as described in 10.8.1.1): a) **MaxFrameSize:** The 16-bit unsigned MaxFrameSize component is used to allocate resources and adjust queue selection parameters in order to supply the QoS requested by an MSRP Talker Declaration. It represents the maximum frame size that the Talker will produce, excluding any overhead for media-specific framing (e.g., preamble, IEEE 802.3 header, Priority/VID tag, CRC, interframe gap). As the Talker or Bridge determines the amount of bandwidth to reserve on the egress port it will calculate the media-specific framing overhead on that port and add it to the number specified in the MaxFrameSize field. b) **MaxIntervalFrames:** The 16-bit unsigned MaxIntervalFrames component is used to allocate resources and adjust queue selection parameters in order to supply the QoS requested by an MSRP Talker Declaration. It represents the maximum number of frames that the Talker may transmit in one "class measurement interval" (34.4). **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is	**34.4 Deriving actual bandwidth requirements from the size of the MSDU** The forwarding and queuing mechanisms defined in this clause use bandwidth parameters that are defined in terms of the actual bandwidth used when frames are transmitted on the medium that supports the MAC Service available through the Port. In contrast, the SRP makes use of a traffic specification (TSpec) for each stream that defines the maximum number of bits per frame (*MaxFrameSize*), of the mac_service_data_unit parameter that is relayed by the relay function of the Bridge, and a maximum frame rate (*MaxIntervalFrames*), in frames per class measurement interval, for that stream; i.e., the TSpec takes no account of the per-frame overhead associated with transmitting the MSDU over a given medium. However, when SRP determines the value to be used for the ***operIdleSlope(N)*** parameter associated with a given queue, it is necessary for this value to include the per-frame overhead that will be incurred when frames are transmitted on that Port. NOTE 1—The frame rate in a TSpec is measured over a "class measurement interval" that depends upon the SR class associated with the stream. SR class A corresponds to a class measurement interval of 125 µs; SR class B corresponds to a class measurement interval of 250 µs. These class measurement intervals apply at the source of the stream, i.e., the "Talker" end station, and do not necessarily hold good for subsequent stages in the stream's transmission across a Bridged Network. For the purposes of calculating the bandwidth consumption of a stream, it is assumed that the stream data is essentially of constant size and transmission rate, so these maxima can be used to directly define an assumed maximum payload size and the maximum frame rate in frames per second; i.e., $assumedPayloadSize = MaxFrameSize \quad (34\text{-}1)$ $maxFrameRate = MaxIntervalFrames \times (1/classMeasurementInterval) \quad (34\text{-}2)$ where *classMeasurementInterval* is measured in seconds. NOTE 2—As stated, the calculation of bandwidth from TSpec parameters assumes that the stream data is essentially of constant frame size, and hence, the approximations shown in this section are valid. If the data varies significantly in frame size, then the calculation of per-frame overhead using these assumptions could be significantly in error. From this, and also from local knowledge of the protocol stack that supports the Bridge Port, it is possible to determine the overhead that is added to the per-frame MSDU payload when a frame is transmitted. There are at least the following sources of per-frame overhead: a) Any VLAN tags and security tags (see IEEE Std 802.1AE) that are added to the layer 2 payload as it passes through the various service interfaces in the Port's protocol stack. b) The MAC framing (header and trailer octets, plus any padding octets that are required to meet minimum frame size limitations) that is added by the underlying MAC Service. c) Any physical layer overhead, such as preamble characters and inter-frame gaps. The precise per-frame overhead will therefore depend upon the protocol stack and the underlying MAC technology. The actual bandwidth needed to support a given stream is therefore defined as follows [using *assumedPayloadSize* from Equation (34-1)]: $actualBandwidth = (perFrameOverhead + assumedPayloadSize) \times maxFrameRate \quad (34\text{-}3)$ **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
checking, via the access control function, without further interrogations at internal transmission nodes of the communications network, whether the use of the service is permitted, the checking performed taking into account an available capacity, which is	The Channel Utilization field is defined as the percentage of time, linearly scaled with 255 representing 100%, that the AP sensed the medium was busy, as indicated by either the physical or virtual carrier sense (CS) mechanism. When more than one channel is in use for the BSS, the Channel Utilization field value is calculated only for the primary channel. This percentage is computed using the formula, Channel Utilization = Integer((channel busy time/(dot11ChannelUtilizationBeaconIntervals × dot11BeaconPeriod × 1024)) × 255), where channel busy time is defined to be the number of microseconds during which the CS mechanism, as defined in 9.3.2.1, has indicated a channel busy indication, dot11ChannelUtilizationBeaconIntervals represents the number of consecutive beacon intervals during which the channel busy time is measured. The default value of dot11ChannelUtilizationBeaconIntervals is defined in Annex C. The Available Admission Capacity field is 2 octets long and contains an unsigned integer that specifies the remaining amount of medium time available via explicit admission control, in units of 32 µs/s. The field is helpful for roaming STAs to select an AP that is likely to accept future admission control requests, but it does not represent an assurance that the HC admits these requests. **Source: https://standards.ieee.org/standard/802_11-2012.html**

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	**The available capacity is determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network. The checking includes determining the Peak Data Rate field, i.e., maximum allowable data rate for transport of MSDUs or A-MSDUs belonging to this TS [traffic streams].** **The "Insufficient QOS capacity for current traffic streams" failure code suggests that the whether the service usage comprising of that particular traffic streams is possible or not and thus is done on the basis of transmission capacity and QOS capacity available.** The Target BSSID field contains the 6-octet BSSID address of the AP that is the target of the attempted Transition. The Transition Time field contains the transition time in TUs. The transition time is defined in 10.23.2.2. The Transition Reason field indicates the reason why a transition attempt occurred and contains one of the values in Table 8-138. **Table 8-138—Transition and Transition Query reasons** (table below) **Source: https://standards.ieee.org/standard/802_11-2012.html**

Transition Reason value	Description
0	Unspecified
1	Excessive frame loss rates and/or poor conditions
2	Excessive delay for current traffic streams
3	Insufficient QoS capacity for current traffic streams (TSPEC rejected)
4	First association to ESS (the association initiated by an Association Request message instead of a Reassociation Request message)
5	Load balancing
6	Better AP found
7	Deauthenticated or Disassociated from the previous AP
8	AP failed IEEE 802.1X EAP Authentication
9	AP failed 4-Way Handshake

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	**5.2.2.4 Effect of receipt** On receipt of this primitive, the MAC sublayer entity determines whether it is able to fulfill the request according to the requested parameters. A request that cannot be fulfilled according to the requested parameters is discarded, and this action is indicated to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive that describes why the MAC was unable to fulfill the request. If the request can be fulfilled according to the requested parameters, the MAC sublayer entity appends all MAC specified fields (including DA, SA, FCS, and all fields that are unique to IEEE Std 802.11), passes the properly formatted frame to the lower layers for transfer to a peer MAC sublayer entity or entities (see 5.1.4), and indicates this action to the LLC sublayer entity using an MA-UNITDATA-STATUS.indication primitive with transmission status set to Successful. **Source: https://standards.ieee.org/standard/802_11-2012.html** The Peak Data Rate field is 4 octets long and contains an unsigned integer that specifies the maximum allowable data rate, in bits per second, for transfer of MSDUs or A-MSDUs belonging to this TS within the bounds of this TSPEC. If p is the peak rate in bits per second, then the maximum amount of data, belonging to this TS, arriving in any time interval $[t1,t2]$, where $t1 < t2$ and $t2 - t1 > 1$ TU, does not exceed $p \times (t2 - t1)$ bits. **Source: https://standards.ieee.org/standard/802_11-2012.html**

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	**34.3.1 Relationships among bandwidth availability parameters** The recommended default value of *deltaBandwidth(N)* for the highest numbered traffic class supported is 75%, and for any lower numbered traffic classes, the recommended default value is 0%. The *deltaBandwidth(N)* for a given *N*, plus the *deltaBandwidth(N)* values for any higher priority queues (larger values of *N*) defines the total percentage of the Port's bandwidth that can be reserved for that queue and all higher priority queues. For the highest priority queue, this means that the maximum value of *operIdleSlope(N)* is *deltaBandwidth(N)*% of *portTransmitRate*. However, if *operIdleSlope(N)* is actually less than this maximum value, any lower priority queue that supports the credit-based shaper algorithm can make use of the reservable bandwidth that is unused by the higher priority queue. So, for queue N-1, the maximum value of (*operIdleSlope(N)* + *operIdleSlope(N-1)*) is (*deltaBandwidth(N)* + *deltaBandwidth(N-1)*)% of *portTransmitRate*. NOTE 1—For example, suppose two queues, 3 and 2, support the credit-based shaper algorithm for SR classes A and B, respectively. Suppose *deltaBandwidth(3)* for SR class A is currently 20%, and *deltaBandwidth(2)* for SR class B is currently 30%. If *operIdleSlope(3)* is currently 10% of *portTransmitRate*, then half of queue 3's maximum allocation is unused, and the maximum value of *operIdleSlope(2)* is therefore currently 40% of *portTransmitRate*. However, if *operIdleSlope(3)* increases to the full 20% that it is entitled to use, the maximum value of *operIdleSlope(2)* reduces to 30% of *portTransmitRate*. NOTE 2—The sum of the *deltaBandwidth(N)* values for all values of N should be chosen such that there is sufficient bandwidth available for any nonreserved (best-effort, strict-priority) traffic; the default values are chosen such that the sum of the *deltaBandwidth(N)* values is 75%, so no more than 75% of the Port's available bandwidth is permitted to be reserved. This ensures that when using default settings, there is at least 25% of the Port's bandwidth available for nonreserved traffic. However, as these default settings may be inappropriate for some situations (e.g., links that offer very high bandwidth, or networks with very low levels of nonreserved traffic), they can be modified by management. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**

Claim 1	RUCKUS DEVICES
determined taking into account the overall transmission capacity, and available to the access node for transmitting traffic streams to the communications network.	**35.2.2.4 MSRP AttributeType definitions** MSRP defines four AttributeTypes (10.8.2.2) that are carried in MRP exchanges. The numeric values for the AttributeType are shown in Table 35-1 and their use is defined by the following list: a) **Talker Advertise Vector Attribute Type:** Attributes identified by the Talker Advertise Vector Attribute Type are instances of VectorAttributes (10.8.1), used to identify a sequence of values of Talker advertisements for related Streams that have not been constrained by insufficient bandwidth or resources. b) **Talker Failed Vector Attribute Type:** Attributes identified by the Talker Failed Vector Attribute Type are instances of VectorAttributes, used to identify a sequence of values of Talker advertisements for related Streams that have been constrained by insufficient bandwidth or resources. c) **Listener Vector Attribute Type:** Attributes identified by the Listener Vector Attribute Type are instances of VectorAttributes, used to identify a sequence of values of Listener requests for related Streams regardless of bandwidth constraints. Listener Vector Attribute Types are subdivided into individual Declaration Types via the MSRP FourPackedEvents (35.2.2.7.2). d) **Domain Vector Attribute Type:** Attributes identified by the Domain Vector Attribute Type are instances of VectorAttributes, used to identify a sequence of values that describe the characteristics of an SR class. **Source: https://standards.ieee.org/standard/802_1Q-2018.html**